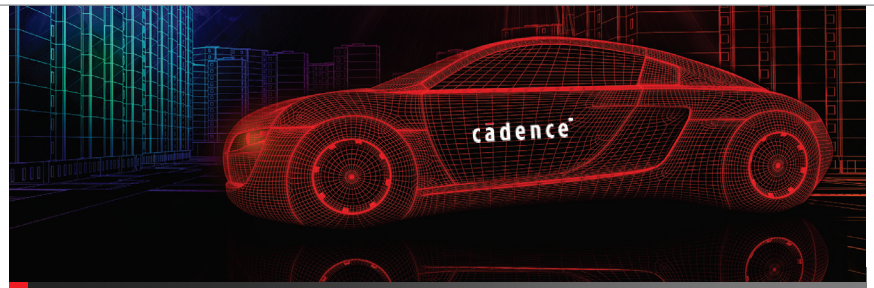
Meeting ADAS SoC Safety Design Challenges with Active Safety Feature-Enabled IP

Cadence Design Systems

ABSTRACT

The automotive industry is going through a fast-paced electronic revolution, driven by higher and higher demand of autonomous vehicles. New vehicles released to market today are already deploying 6-10 ADAS modules with various sensors capable of supporting semi- or high- automation levels defined by NHTSA. However, challenges remain to unleash the power of technology due to safety concerns. Due to high computation demand and the need to support multiple sensors, ADAS SoC is extremely complex to design and requires most advanced semiconductor processing nodes. Semiconductor vendors and Tier-1 suppliers attempting to develop ADAS ASICs must rely on IP suppliers to achieve silicon success. IPs designed using traditional safety methodology may achieve the goal of stringent level functional safety standards but are no longer sufficient to meet the real-time safety decisions required in current and future ADAS SoCs. To design effective functional safety mechanism at SoC level, the internal logic of the ADAS optimized IPs need to incorporate additional functionalities to offload and complement the complexities in the system design. Cadence has been working with automotive semiconductor vendors and Tier-1 suppliers to ensure that IPs are meeting functional safety requirements defined by ISO26262 standard. We added active functional safety mechanisms as differentiating features into the IPs. These features are documented in the functional safety manuals. In this presentation, we will highlight the representative functional safety features that have been instrumented in various IPs, their impact to SoC level functional safety architecture, and the ISO26262 FMEDA evaluation process to quantify the effectiveness of these features.



Meeting ADAS SoC Safety Design Challenges with Active Safety Feature-Enabled IP

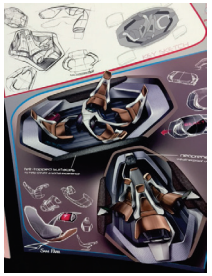
Charles Qi, Sr. Design Engineering Architect
IPG System Engineering
TSMC OIP
September 2017

cadence

Self-Driving Car: Vision and Reality

The automotive industry is facing radical changes

Poster at 2015 SAE Congress: Future Self-Driving Car



No active driver,
100% machine-controlled

Tesla Model S Autopilot

source: wallstreetpit.com

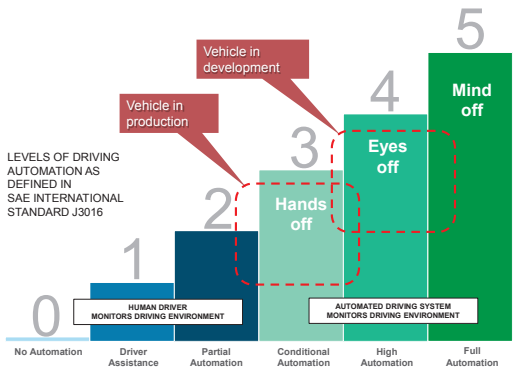
Partial ADAS in production,
Over 130 million real road miles

cadence

Roadmap to Autonomous Driving

"With great power comes great responsibility"

- Amount of electronics is growing fast (with the level of automation)
- Advanced driver assistance systems (ADAS) are based on complex SoCs
- Safety critical applications have stringent requirements on
  - Functional Safety
  - Reliability
  - Security



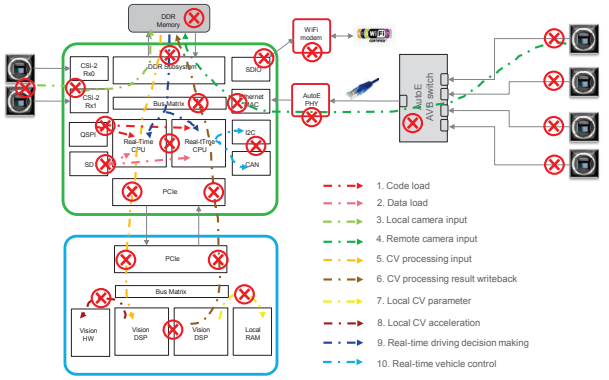
cadence

Safety Design Challenges

Complex data flow, many failing points in ADAS chip-set

Application Processor

Vision Processor



cadence

Failure Modes and Impacts of ADAS SoCs

Component	Failure Mode	Impact on System Safety Goals
Local camera/interface	CMOS sensor interface malfunction Image sensing stopped Noisy or distorted image frames Missing pixel/line/frames	Unable to detect road obstacles Unable to detect and recognize traffic signs Unable to detect driving path
Remote camera network	Faulty or interrupted image streams	Unable to detect road obstacles Unable to detect and recognize traffic signs Unable to detect driving path
In-car data network	Faulty communication of data or control	Incorrect or mistimed sensor fusion data or vehicle control data Incorrect or mistimed driving decision
DDR memory	Corruption of memory content	Corruption of code/operation parameters/image data result to incorrect driving decisions
DDR subsystem	Incorrect training or calibration Control state corruption Local buffer corruption Datapath data/address bus error	Corruption of code/operation parameters/image data result to incorrect driving decisions
Data transfer over PCI Express® (PCIe®) for CV processing	PCIe physical link error Incorrect TX/RX PCIe transactions Stuck or overflow/underflow Local buffer corruption Datapath data/address bus error	Incorrect or incomplete image data transfer Incorrect or incomplete computation control Incorrect or incomplete computation result transfer Result in false detection/mis-detection or lockup of operations
CV DSP/Hardware	Computation error in ADAS CV DSP processing	False detection/mis-detection or lockup of operations
Real-time CPU	Computation error in processor ADAS driving decision code execution due to processor internal state corruption	Incorrect driving decision Incorrect or untimely control command
Code/data flash	Corruption of ADAS application code or non-volatile data used for ADAS operations (e.g., CNN parameters)	Incorrect driving decision Incorrect or untimely control command Completely lockup or non-operational
Real-time control peripherals	Malfunction of control peripherals	Unable to issue control command Corrupted command/control data or incorrectly target recipient

Safety Design for ADAS

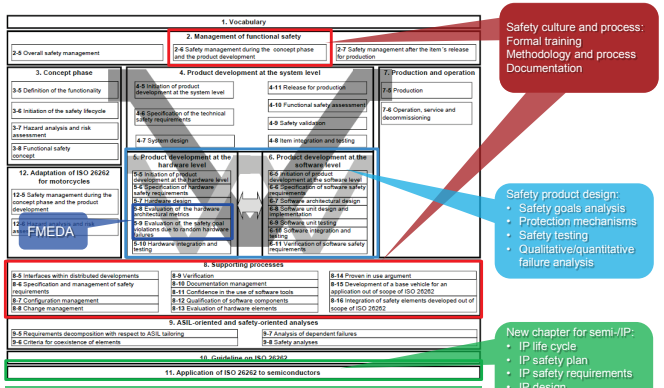
Observations based on customer demands

Increased Safety Impact
- Safety is non-optional at levels 4-5 because machines are performing real-time vehicle control
- Safety failure results in fatalities, recalls, and lawsuits
- Vehicle must be fail-operational or not fail at all

Safety Is Designed in Early
- Complex safety architecture, increasing number of safety mechanisms
- No assurance of system safety with blackbox components designed without safety principles
- After-thought protection mechanisms are not fail-operational

Safety Analysis and Verification
- FMEDA analysis is no more sufficient for complex SoCs
- SoC FIT error rate estimation is challenging
- Fault injection to enable fault classification at IP and SoC level

Dissecting ISO 26262: Implications to IP



Safety culture and process:
- Formal training
- Methodology and process
- Documentation

Safety product design:
- Safety goals analysis
- Protection mechanisms
- Safety testing
- Qualitative/quantitative failure analysis

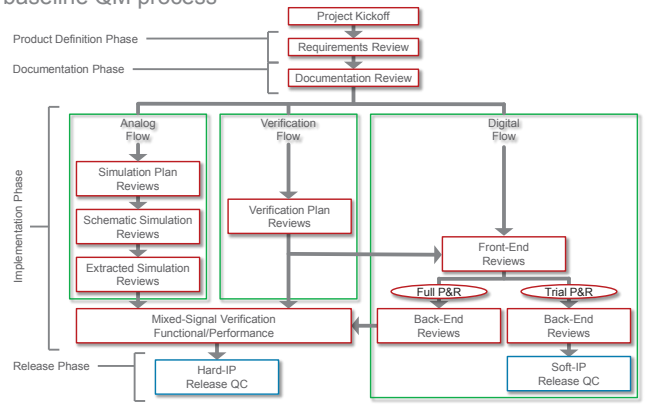
New chapter for semi-/IP:
- IP life cycle
- IP safety plan
- IP safety requirements
- IP design
- IP evaluation
- IP supporting evidence

ISO 26262 Edition 2, Part 11

IP are typically developed as safety element out of context (SEooC), however IP safety assurance and awareness impact overall system safety

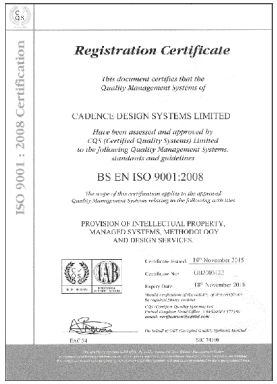
Establish Formal Quality Flow and Checkpoints

Establish baseline QM process



Ensure Quality via ISO 9001

Formal site evaluation



cadence

Active Safety Mechanisms Under Consideration

A summary of effective hardware safety mechanisms

Memory Protection
- ECC for RAM
  - 1-bit correction
  - 2-bit detection
- Parity for RAM/flash
- Checksum for ROM

State Protection
- Parity for CSRs
- Redundancy for CSRs
- Redundancy for FSM state encoding
- Illegal state detection

Datapath Protection
- Data bus ECC
- Data bus parity
- Address bus parity
- FIFO overflow underflow
- Anti-lockup watchdog

Communication Protection
- PHY-layer BER checking
- Error correction coding
- Link-layer CRC/FCS
- Transaction-layer CRC
- Header CRC/checksum
- Illegal format detection

BIST
- Logic BIST (test during runtime)
- Memory BIST
- PRBS and loopback
- Known answer test

Electrical Reliability
- Analog operating point calibration
- BER calibration
- Timing calibration and training
- Voltage, temperature monitor

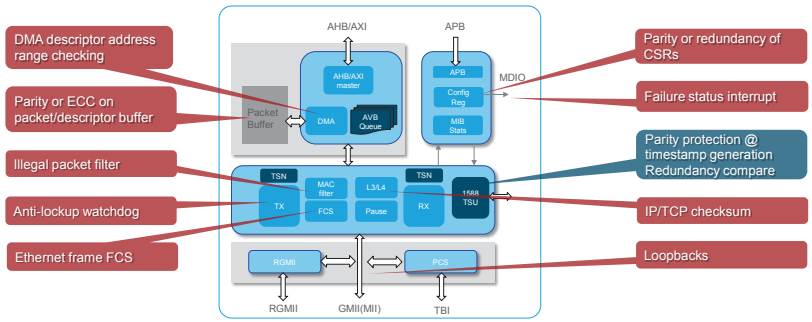
Failure Notification
- Failure notification pin
- Failure notification interrupt
- Failure status CSR and event logging counters

Failure Recovery
- Software/hardware reset
- Software/hardware initiated recalibration
- Self correction through error correction code

cadence

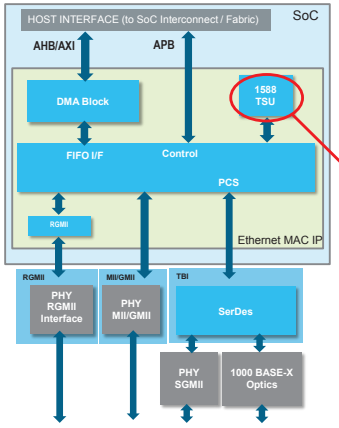
Active Safety Features in Automotive Ethernet MAC IP

Enables deterministic, real-time data transfer for safety-critical applications



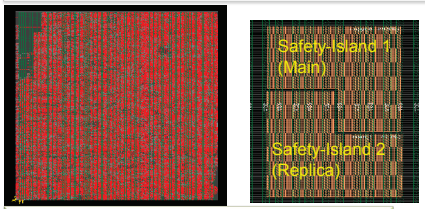
cadence

Safety-Aware P&R of the Automotive Ethernet MAC/PCS IP



- Provides the logic required to integrate a Gigabit Ethernet MAC and 1000BASE-X PCS into any SoC
- Enables deterministic, real-time data transfer for safety-critical applications supporting the Time Sensitive Network Protocol (IEEE 802.1as / 1588)
- Certified as ASIL-B ready

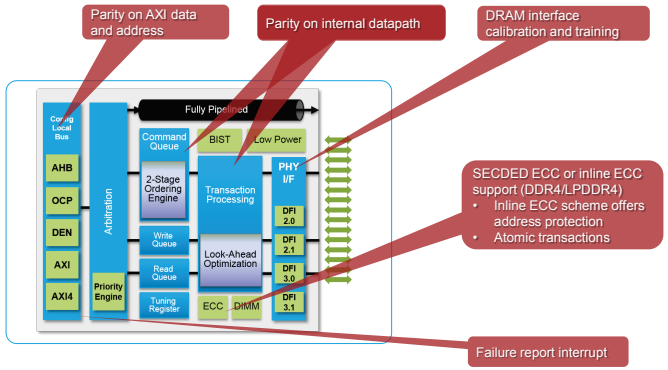
- Time Stamp Unit (TSU) is key to the TSN standard
- TSU output protection identified during FMEDA as key to improve FS
- TSU block duplicated and provided instant detection of faults (automatic comparison of each of the TSU's timer output, on a cycle-to-cycle basis)



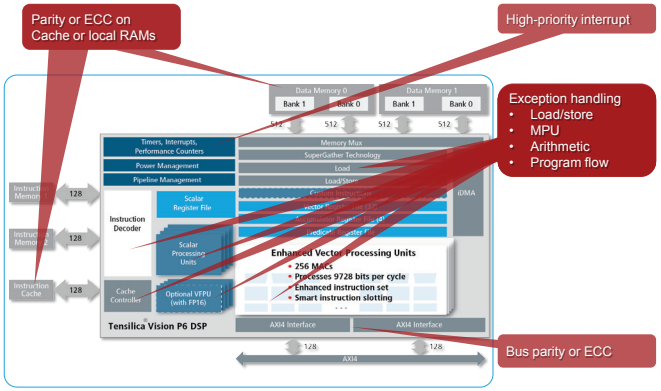
TSMC 16FF, Instance Count: ~150K, Design Utilization ~ 70%

cadence

Active Safety Features in DDR Controller IP

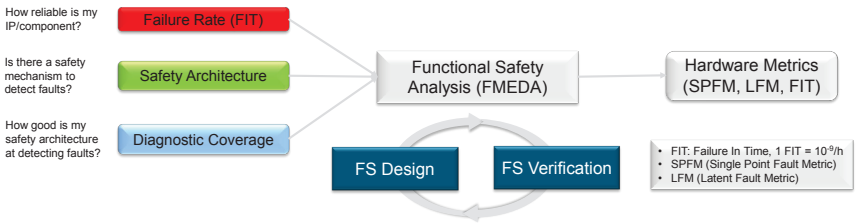


Active Safety Features in Tensilica Vision DSP Processor



Functional Safety Analysis and Verification

Understanding and achieving ASIL hardware metrics

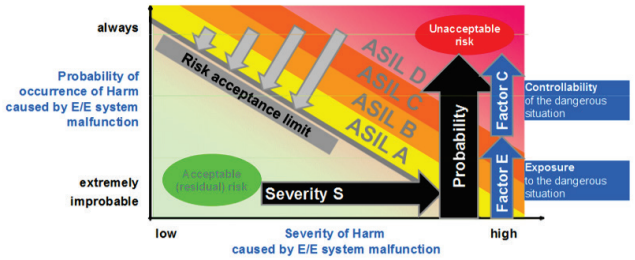


ASIL	Failure Rate	SPFM	LFM
A	< 1000 FIT	Not relevant	Not Relevant
B	< 100 FIT	≥ 90%	≥ 60%
C	< 100 FIT	≥ 97%	≥ 80%
D	< 10 FIT	≥ 99%	≥ 90%

Functional Safety analysis
- Structured approach to measure the hardware metrics
- Drives the design/verification steps to achieve such metrics

Quantifying Safety by ASIL Levels

Chance of exposure, severity, and controllability



A Close Look at FMEDA – Faults and Metrics

Impact of safety mechanism to failure mode classification

Safe fault (λ_s)
→ Fault that leads to a safe condition or has no impact on the respective safety goal

Detected multiple point fault ($\lambda_{MPF\ detected}$)
→ Detected multiple fault
→ No safety goal violation

Perceived multiple point fault ($\lambda_{MPF\ perc.}$)
→ Multiple fault detected by the driver
→ No safety goal violation

Single point fault (λ_{SPF})
→ Undetected single fault
→ Leads to safety goal violation Fault Tolerance Time to be considered

Residual fault (λ_{RF})
→ Partially not detected single fault (due to diagnostic slip)
→ Leads to safety goal violation , Fault Tolerance Time to be considered

Latent multiple point fault ($\lambda_{MPF\ latent}$)
→ Undetected multiple fault
→ Leads to safety goal violation in combination with another independent fault

Faults in logic functions protected by safety mechanism can be re-classed from SPF to MPF

$$\text{Single Point Fault metric} = 1 - \frac{\sum_{\text{Safety related HW elements}} (\lambda_{SPF} + \lambda_{RF})}{\sum_{\text{Safety related HW elements}} \lambda}$$

$$\text{Latent Fault metric} = 1 - \frac{\sum_{\text{safety related HW elements}} (\lambda_{MPF\ Latent})}{\sum_{\text{safety related HW elements}} (\lambda - \lambda_{SPF} - \lambda_{RF})}$$

	ASIL B	ASIL C	ASIL D
Single Point Fault Metric (SPFM)	>= 90%	>= 97%	>=99%
Latent Fault Metric (LFM)	>= 60%	>= 80%	>= 90%

ISO 26262-5, Table 4 + 5

Fault metric targets for latent multi-point faults are much lower for ASIL levels

cādence

A Close Look at FMEDA – Safety Goal Analysis

Determine probability of failures leading to safety goal violation

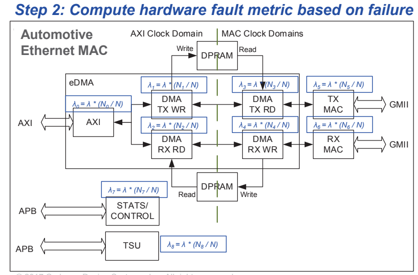
Step 1: Nominal IC failure rate calculation according to IEC TR 62380 (2004-08)

MATHEMATICAL MODEL :

$$\lambda = \left(\underbrace{\left\{\lambda_1 \times N \times e^{-0.35 \times a} + \lambda_2\right\} \times \left\{\frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}}\right\}}_{\lambda_{die}} + \underbrace{\left\{2.75 \times 10^{-3} \times \pi_\alpha \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68}\right) \times \lambda_3\right\}}_{\lambda_{package}} + \underbrace{\left\{\pi_I \times \lambda_{EOS}\right\}}_{\lambda_{overstress}} \right) \times 10^{-9} / h$$

N: total transistor count
a: years in operation
λ1: per transistor failure rate
λ: FIT rate for entire IP

Step 2: Compute hardware fault metric based on failure distribution and diagnostic coverage



Distribute to sub-modules based on gate count
$\lambda_i = \lambda * (N_i / N)$

Compute metrics (SPFM and LFM) based on fault classification and diagnostic coverage for all sub-modules

$\lambda_{i\ RF} = \lambda_{i\ SPF} * (1 - DC_i)$
$\lambda_{i\ MPF\text{-}L} = \lambda_{i\ MPF} * (1 - DC_i)$

Aggregate to get overall metrics number and check against ASIL targets

cādence

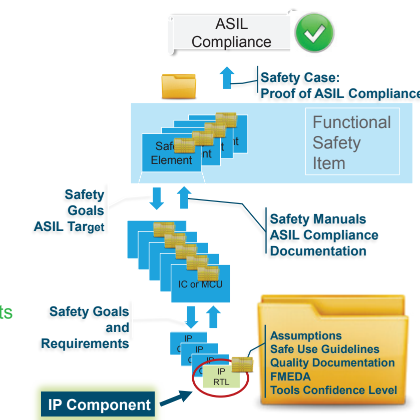
Automotive Ethernet MAC Certified ASIL-B Ready

cādence

Achieving Proof of Compliance with IP Collaterals

Enabling customers to achieve ASIL targets

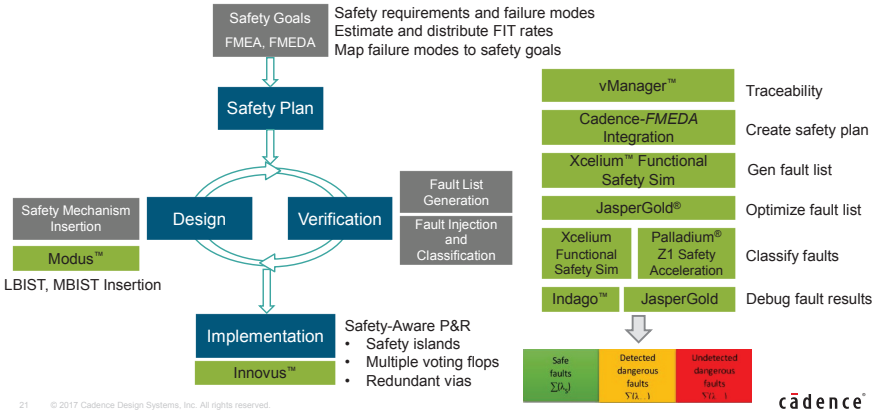
- IP are developed as SEooC
  - Evaluation will be typically to ASIL B level
- ASIL compliance requires
  - Quality management process/certification
  - Safety manual for SEooC
  - Safety features description
  - Failure mode effect and diagnostic analysis
  - Automotive Safety Kits (tools/flows)
- Cadence provides all required documents to our customers to meet their ISO 26262 design targets



cādence

Safety-Aware Design Methodology for IP and SoCs

Design, analysis, verification, and implementation

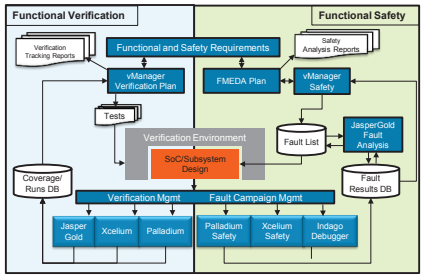


cadence

From Functional Verification to Functional Safety Verification

- Comprehensive integrated functional safety solution
  - I/F to Requirement Management and Tracing tools
  - FMEDA integration with ANSYS Medini
  - Safety verification tightly integrated with functional verification flow
  - vManager platform controls all execution engines
  - Unified fault results DB
- Different types of execution engines for fault classification:
  - Xcelium fault simulation engine → short tests, regressions
  - Hardware-accelerated engine (Palladium) → full-chip, software tests
  - Formal methods (Jasper Gold) → Fault testability and propagation analysis for fault list optimization
- Benefit
  - Comprehensive fault classification to get more realistic FIT numbers for the FMEDA analysis
    → More accurate safety analysis including report

Automotive Functional Safety Verification Solution



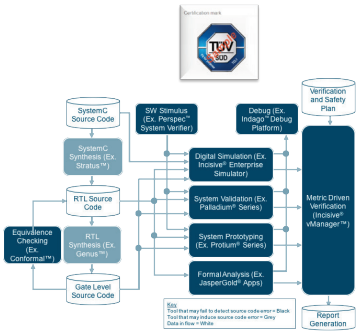
Diagnostic coverage to calculate the hardware metric

cadence

ISO 26262 Process Compliance

Automotive Functional Safety Kits

- Cadence sub-flows compliant to ISO 26262
- Tool-chain and safety manuals audited by TÜV-SÜD and determined "Fit for Purpose"
  - Analog/Mixed-Signal Design and Verification
  - Digital Front-End Design and Verification
  - Digital Implementation and Signoff
  - Silicon Package Board
- Cadence Automotive Safety Kit
  - Flow Safety Manual + Tool Classification Analysis + TÜV-SÜD report
  - Confirmed by **TÜV-SÜD** to be ISO 26262 compliant
  - Can be used/tailored by customers
- Safety kits available for download on cadence.com



Front-End Design and Verification Flow

cadence

Summary

Safety-aware IP and design flow is key to ASICs for autonomous driving

Significantly increased safety requirements on IP
- Complexity is increasing for devices in autonomous driving
- Many possibility of failing points may result in safety goal violations
- Safety needs to be planned early and designed in for IP

ISO 26262 governs IP safety design flow
- Establish formal and certifiable quality management
- Implement active safety protection features in IP
- Systematic failure analysis to meet ASIL requirements
- Apply qualified safety design tools

IP active safety features ensure effective SoC-level safety
- Failures can be detected with high coverage and low latency
- Easy to implement localized diagnostics for higher failure metrics target
- Sensible active safety features in IP reduce SoC-level safety design effort

cadence